REMARKS/ARGUMENT

This Amendment and the following remarks are intended to fully respond to the Final Office Action mailed April 21, 2008, hereinafter "Office Action". In that Office Action claims 1-9, 18-22, and 26-27 were examined, and all claims were rejected. More specifically, claims 1-9, 18-22, and 26-27 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Faucher (USPN 5,515,441), hereinafter "Faucher" in view of Inoue et al. (USPN 6,170,057), hereinafter "Inoue."

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested.

In this Response, claims 1, 3, 5-8, 18, 20-22, and 26-27 have been amended and no claims have been added or canceled. Therefore, claims 1-9, 18-22, and 26-27 remain present for examination.

Claim Rejections – 35 U.S.C. § 103(a)

Claims 1-9 and 18-22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Faucher in view of Inoue. Applicants respectfully traverse the § 103(a) rejections because either the Examiner failed to state a *prima facie* case of obviousness or the current amendments to the claims now render the Examiner's arguments moot. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Further, under *KSR Int'l Co. v. Teleflex, Inc.*, there "must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." 127 S. Ct. 1727, 1741 (2007). Neither Faucher nor Inoue, either separately or in combination, teach or suggest all of the limitations of the recited claims.

Faucher relates to a communication system in which a node may communicate over insecure channels by securing communications. Communications are secured by computing a first cryptovariable from information associated with certificates exchanged between a node and a terminal, computing a second cryptovariable using public key exchange, and computing a

session cryptovariable as a function of the first and second cryptovariables. (Faucher, Abstract, *See also* col. 9, l. 6 – col. 10, l. 16).

Faucher fails to teach or suggest, at least, wherein at least one message that comprises at least part of the IKE quick mode negotiation is sent during the IKE main mode negotiation and a quick mode pseudo random number is exchanged between the responder and the initiator, as recited in independent claim 1. The Office Action states,

> Examiner would like to point to Column 10, lines 13-16 of Faucher reference which recites, "The procedure continues with a straight Diffie-Hellman key exchange to generate a second session key. These two session keys are combined to form the final session key" Applicant should note that the first session key exchanged during main mode is actually needed to derive the final session key. Examiner is interpreting the Diffie-Hellman key exchange and the generation of the final key as a quick mode, it can be seen that the generation of final key requires a first session key exchanged during the main mode negotiation. Therefore, Faucher still discloses the limitation of "wherein at least one message that comprises at least part of the quick mode negotiation is sent during the main mode negotiation and a quick mode pseudo random number is exchanged between the responder and the initiator".

Applicants respectfully disagree with the Examiner's interpretation of what Faucher teaches. Faucher teaches generating a first session key through the exchange of certificates between two terminals. (*See Faucher*, col. 10, ll.2-8). *After* the first key is generated, the reference teaches generating a second key using a Diffie-Hellman key exchage. (*See id.*, col. 10, ll. 13-15). *After* generating the second key, Faucher teaches generating a final key that is a combination of the first and second keys. (*See id.*, col. 10, ll. 15-16). Thus, the reference teaches three distinct processes: generating a first session key, generating a second session key, and generating a final session key. Aside from using the *results* from the first two processes there is no overlap between the processes. Conversely, claim 1 recites a method in which an overlap occurs between the main mode and the quick mode, namely at least **one message** that comprises at least **part of the IKE quick mode** negotiation is **sent during the IKE main mode** negotiation.

Clearly, Faucher with its three *distinct and separate* steps cannot teach or suggest the method as recited in claim 1.

Inoue fails to compensate for Faucher's deficiencies. Inoue relates to a packet encryption and authentication method capable of controlling an activation of a packet encryption and authentication device belonging to a mobile computer. The device is controlled according to the security policy of the network that the mobile computer is visiting. (*See* Inoue, Abstract). Inoue teaches that when a mobile computer recognizes that it is located outside of its home network, it acquires the security parameters associated with the gateway of the home network and the security parameters of the gateway associated with the network currently being visited by the mobile computer. (*See* Inoue, col. 7, ll. 20-27). As such, Inoue also fails to disclose a main mode or quick mode negotiation at all, and therefore cannot be used to overcome Faucher's failure to teach at least **one message** that comprises at least **part of the IKE quick mode** negotiation is **sent during the IKE main mode** negotiation. In light of at least these deficiencies, claim 1 is allowable over the cited references.

Furthermore, even if Faucher did teach an overlap in processes, the reference still fails to teach or suggest the claimed limitations because, as previously asserted by the Applicants in response to at least the last Office Action, the reference does not teach a main mode and a quick mode. Applicants have amended claims 1, 3, 5-8, 18, 20-22, and 26-27 to clarify even further that the claims refer to and IKE main mode and an IKE quick mode. Indeed, Applicants have amended independent claims 1, 18, 26, and 27 to now recite an internet key management and exchange protocol (IKE) main mode negotiation and an internet key management and exchange protocol (IKE) quick mode negotiation. The MPEP states that the PTO may interpret "the scope of claims in patent applications not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction 'in light of the specification as it would be interpreted by one of ordinary skill in the art.'" (MPEP § 2111 (citing *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364[, 70 USPQ2d 1827] (Fed. Cir. 2004))). Applicants respectfully submit that the Office Action's interpretation of the Diffie-Hellman key exchange plus calculation of the final key in Faucher as the quick mode is unreasonable in light of the specification and the claims as amended.

Indeed, during an IKE main mode negotiation an initiator and a responder establish an IKE security association (SA) in order to create a secure channel for IKE negotiations. (*See* Specification, p. 2, ll. 12-19). An IKE quick mode negotiation is used to negotiate general purpose SAs over the secure channel negotiated during the IKE main mode. The portion of Faucher relied upon by the Office Action only teaches generating various keys, not establishing a secure channel and then negotiating general purpose SAs over the secure channel. Clearly, the cited portion of the reference fails to teach or suggest the claimed method of performing and IKE main mode negotiation and a IKE quick mode negotiation. For at least this additional reason, the cited references cannot teach or suggest the limitation of the recited claims.

For at least similar reasons, independent claim 18 is also allowable over the cited references. Claim 18 recites, *inter alia*, wherein at least one message that comprises at least part of the IKE quick mode negotiation is sent during the IKE main mode negotiation and a quick mode pseudo random number is exchanged between the responder and the initiator.

Similarly, independent claim 26 is also allowable over the cited references. Claim 26 recites, *inter alia*, receiving, at the initiator, a second message, wherein the second message comprises at least part of the IKE main mode negotiation and at least part of an internet key management and exchange protocol (IKE) quick mode negotiation and the IKE quick mode negotiation comprises deriving a set of keys usable with the security protocol.

Finally, for at least similar reasons, independent claim 27 is also allowable over the cited references. Claim 27 recites, *inter alia*, sending, from the responder, a second message, wherein the second message comprises at least part of the IKE main mode negotiation and at least part of an internet key management and exchange protocol (IKE) quick mode negotiation and wherein the IKE quick mode negotiation comprises deriving a set of keys usable with the security protocol.

For at least the forgoing reasons, neither Faucher nor Inoue, alone or in combination, teach all of the limitations of independent claims 1, 18, 26, and 27 and, therefore, the claims are allowable over the references of record. All other claims, *i.e.*, claims 2-9 and 19-22 depend from one of the allowable independent claims and are, thus, also allowable over the cited references. Applicants respectfully request that the Examiner issue a notice of allowance, for all claims, at

his earliest convenience.

Conclusion

This Amendment fully responds to the Office Action mailed on April 21, 2008. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicant believes the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the art of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Dated: May 15, 2008

Gregory D. Leibold, Reg. No. 36,408
Merchant & Gould P.C.
PO Box 2903
Minneapolis, MN 55402-0903
303.357.1642